CLAIMS

1. An apparatus for generating a random number, comprising:

a first variable frequency oscillator, for generating a first oscillatory signal at a first frequency;

a second variable frequency oscillator, for generating a second oscillatory signal that is asynchronous to said first oscillatory signal and having a second frequency less than said first frequency, wherein bits of the random number are configured from samples of said first oscillatory signal taken at said second frequency; and

frequency variation logic, coupled to said second variable frequency oscillator, for generating a noise signal that directs said second variable frequency oscillator to vary said second frequency, wherein said noise signal corresponds to a parity comparison of a third oscillatory signal and a fourth oscillatory signal, said third and fourth oscillatory signals being asynchronous to each other and to said first and second oscillatory signals.

2. The apparatus as recited in claim 1, wherein said first and second variable frequency oscillators comprise ring oscillators within an integrated circuit.

3. The apparatus as recited in claim 1, wherein said first frequency is at least two times said second frequency.

4. The apparatus as recited in claim 1, wherein the random number comprises eight of said bits.

5. The apparatus as recited in claim 1, wherein said parity comparison comprises an exclusive-OR logic comparison of logic states of said third and fourth oscillatory signals.

6. The apparatus as recited in claim 1, further comprising:

a variable bias generator, for providing a bias signal to said first and second oscillators and to said frequency variation logic, wherein said first frequency, a range for said second frequency, and corresponding frequencies for said third and fourth oscillatory signals are set according to said bias signal.

7. The apparatus as recited in claim 6, wherein a plurality of said bits of the random number are provided to said variable bias generator, and wherein said variable bias generator varies said bias signal according to states of said plurality of said bits.

8. The apparatus as recited in claim 7, wherein a first state of said noise signal directs said second variable frequency oscillator to vary said second frequency to a minimum frequency achievable in accordance with said bias signal, and a second state directs said second variable frequency oscillator to vary said second frequency to a maximum frequency achievable in accordance with said bias signal.

9. The apparatus as recited in claim 1, further comprising:

balance logic, coupled to said second variable frequency oscillator, for examining successive pairs of said samples, wherein said balance logic configures said bits of the random number only from ones of said successive pairs whose two member samples have different states.

10. The apparatus as recited in claim 9, further comprising:

parallel conversion logic, coupled to said balance logic, for aggregating said bits into the random number, and for providing an indication that the random number has been configured.

11. A random number generation apparatus for use within an integrated circuit, comprising:

a fast oscillator, configured to generate a fast oscillatory signal at a first frequency;

a slow oscillator, configured to generate a slow oscillatory signal, the slow oscillatory signal being decoupled from said fast oscillatory signal and being at a second frequency that is less than half of said first frequency;

domain synchronization logic, coupled to said fast and slow oscillators, configured to sample said fast oscillatory signal in phase with said slow oscillatory signal to obtain potential bits for a random number; and

frequency variation logic, coupled to said slow oscillator, configured to vary said second frequency based upon a logical comparison of states corresponding to two independent oscillatory signals.

12. The random number generation apparatus as recited in claim 11, wherein said fast and slow oscillators comprise ring oscillators.

13. The random number generation apparatus as recited in claim 11, wherein said random number comprises eight bits.

14. The random number generation apparatus as recited in claim 11, wherein said frequency variation logic executes an exclusive-OR logical comparison of said two independent oscillatory signals.

15. The random number generation apparatus as recited in claim 11, further comprising:

a bias generator, configured to generate a bias signal that is distributed to said fast and slow oscillators and to said frequency variation logic, wherein said first frequency, a range for said second frequency, and corresponding frequencies for said two independent oscillatory signals are set according to said bias signal.

16. The random number generation apparatus as recited in claim 15, wherein a plurality of bits from said random number are employed by said bias generator to vary said bias signal according to states of said bits.

17. The random number generation apparatus as recited in claim 16, wherein said frequency variation logic generates a noise signal, and wherein one state of said noise signal directs said slow oscillator to vary said second frequency to a minimum frequency corresponding to said bias signal, and an alternative state directs said slow oscillator to vary said second frequency to a maximum frequency corresponding to said bias signal.

18. The random number generation apparatus as recited in claim 11, further comprising:

balance logic, coupled to said slow oscillator, for examining successive pairs of said potential bits, wherein said balance logic configures said bits of said random number only from ones of said successive pairs whose two potential bits have different states.

19. The random number generation apparatus as recited in claim 18, further comprising:

parallel conversion logic, coupled to said balance logic, for aggregating said bits into said random number, and for indicating availability of said random number.

20. A random number generator within a microprocessor, comprising:

a slow oscillator, for producing a sampling clock signal, wherein said sampling clock signal is employed to obtain samples of a first oscillatory signal, and wherein said sampling clock signal runs at less than half the frequency of said first oscillatory signal;

balance logic, coupled to said slow oscillator, for rejecting successive pairs of said samples that have the same state, and for configuring bits of a random number from said successive pairs of said samples that have different states; and

frequency variation logic, coupled to said slow oscillator, for comparing logic states of two asynchronous oscillatory signals, and for varying said frequency of said sampling clock signal according to a noise signal that corresponds to an exclusive-OR function of said logic states.

21. The random number generator as recited in claim 20, wherein said random number comprises eight of said bits.

22. The random number generator as recited in claim 20, further comprising:

a bias generator, for generating a bias signal that is distributed to said slow oscillator and to said frequency variation logic, wherein, according to said bias signal, a frequency range of said sampling clock signal and corresponding frequencies for said two asynchronous oscillatory signals are set.

23. The random number generator as recited in claim 22, wherein said bias generator receives a plurality of said bits from said random number, and wherein said bias generator varies said bias signal according to states of said bits.

24. The random number generator as recited in claim 23, wherein one state of a noise signal provided by said frequency variation logic directs said slow oscillator to vary the frequency of said sampling clock signal to a minimum frequency corresponding to said bias signal, and an alternative state directs said slow oscillator to vary the frequency of said sampling clock signal to a maximum frequency corresponding to said bias signal.

25. The random number generator as recited in claim 20, further comprising:

parallel conversion logic, coupled to said balance logic, for aggregating said bits into said random number, and for providing an indication that said random number is configured.